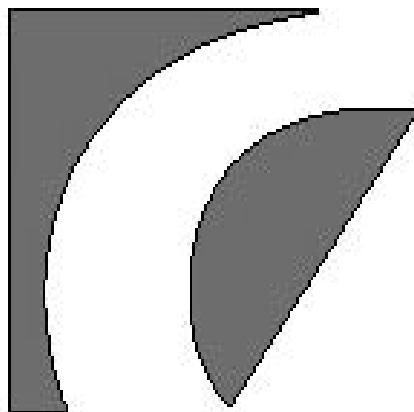
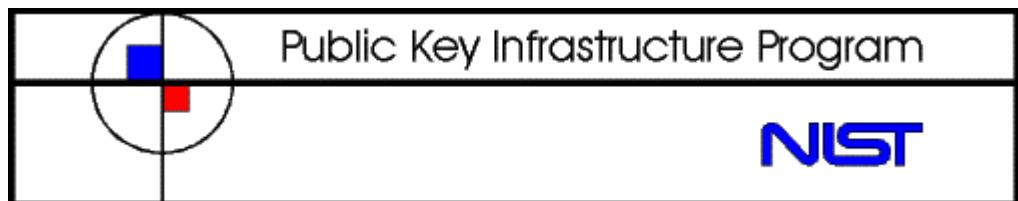


# Directory Security Brief



# Chromatix

8 October 1998  
Steven.Peterson@Chromatix.com

# AGENDA

---

- Chromatix Directory Experience
- Directory Security
- Lessons Learned
- SafePages Directory Suite

# CHROMATIX DIRECTORY EXPERIENCE

---

- 1991 - DMS Directory management research project. Used Isode based products. Produced the first graphical Administrative Directory User Agent (ADUA)
- 1993 - Integrated Strong Authentication into ADUA and DSA for the NSA MISSI Directory Prototype Effort
- 1993 - Developed Secure LDAP (SLDAP) for use in DUA for low end PCs
- 1997 - LDAP/X.500 Directory Products (SafePages™ Directory Suite) Commercially Available



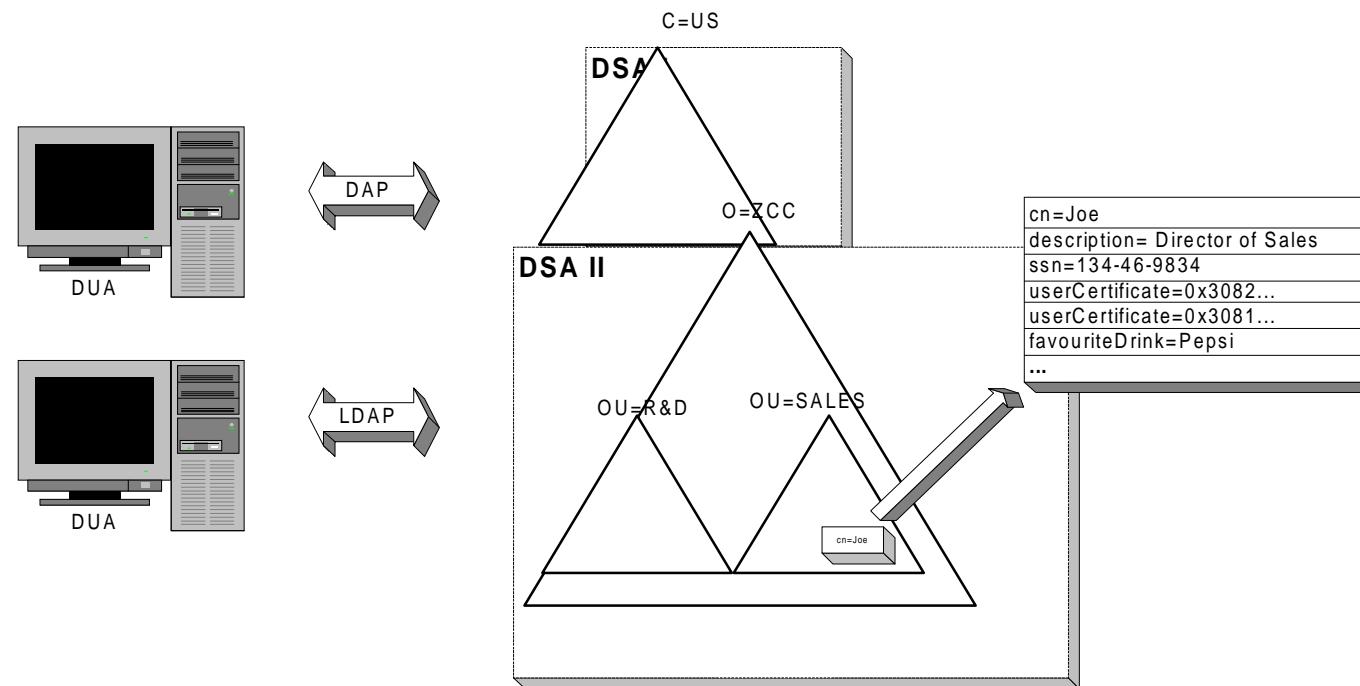
# DIRECTORY SECURITY

# DIRECTORY SECURITY

---

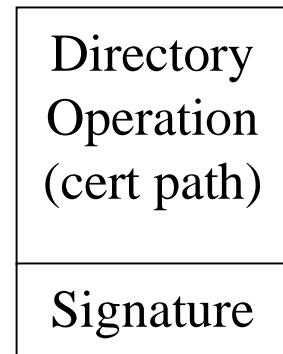
- X.501 ACIs (Access Control Items)
- X.511 Signed Operations (X.509 V1/V3 Certs, V1/V2 CRLs)
- X.511 vs. SSL/TLS
- X.518 Signed DSP (Directory System Protocol)
- X.525 Signed DISP (Directory Information Shadowing Protocol)
- Secure LDAP (SLDAP)
- Directory Threats

# X.501 ACIs

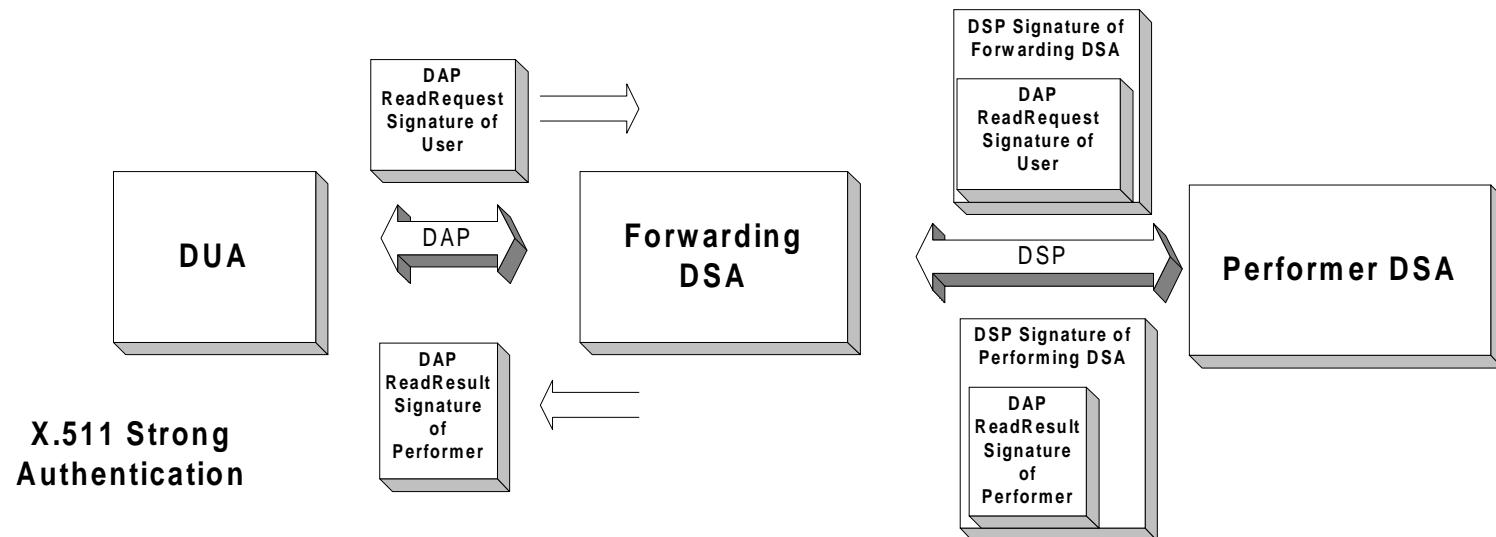


# Signed Directory Operation

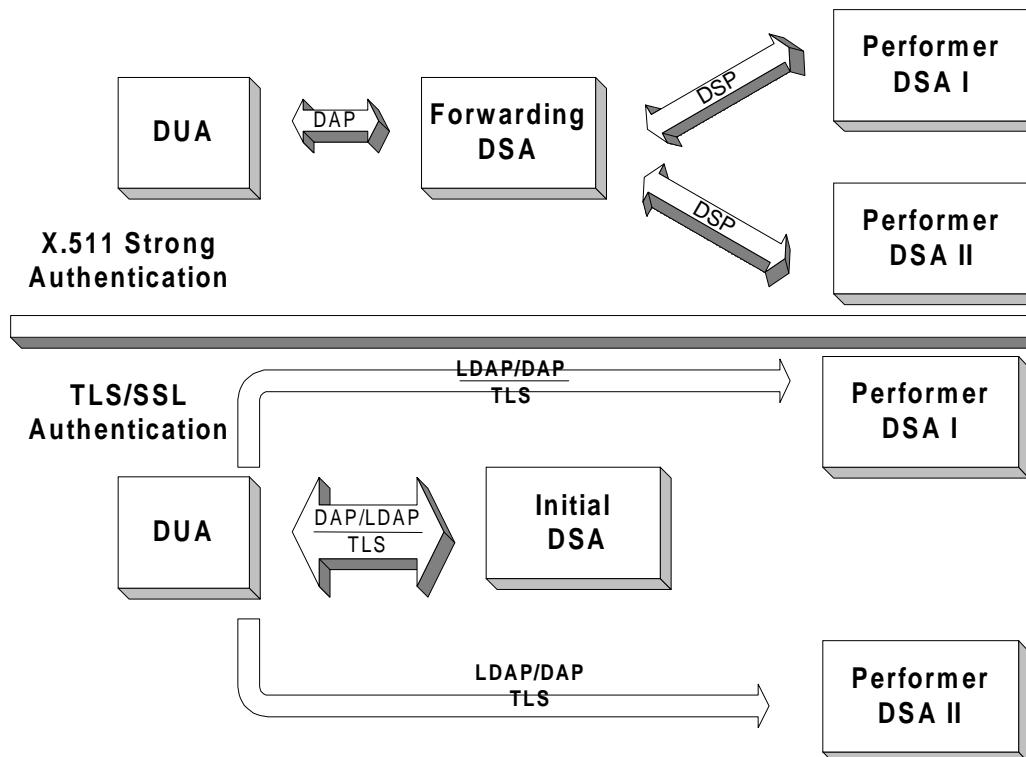
- Sender
  - Hash Directory Op (SHA-1, MD5) yields Hash
  - Sign the Hash w/ sender's private key (DSA, RSA) yields Signature
- Receiver
  - Verify Cert Path (validate path, check CRLs), cache
  - Hash Directory Op (sender's hashing alg)
  - Verify Signature w/ sender's public key (sender's signature alg)



# X.511 Signed Operations

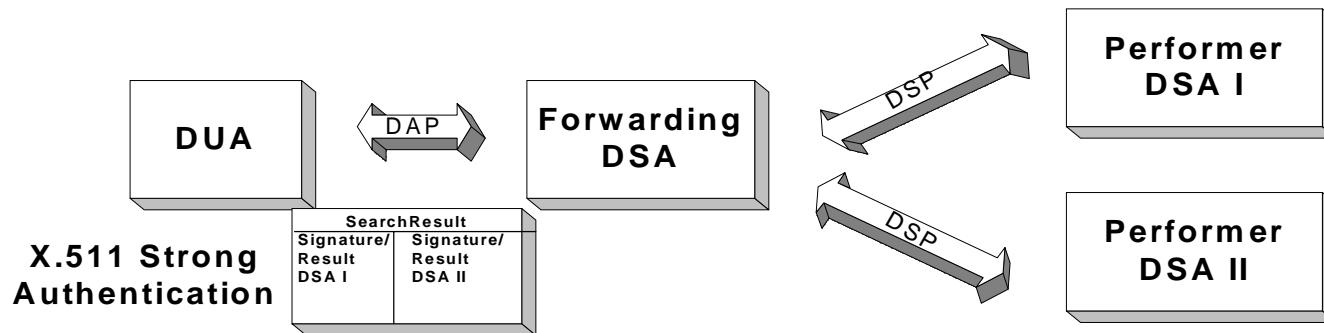


# X.511 Signed Operations vs SSL/TLS

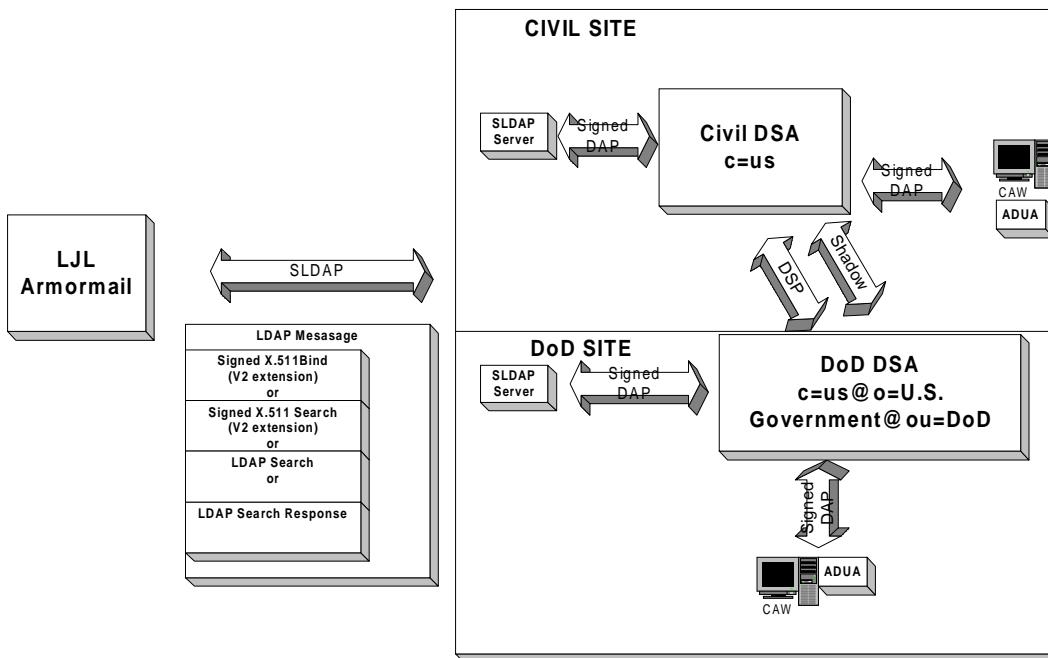


# X.518 Signed DSP

Verifying signatures on search results obtained from multiple performing DSAs



# Secure LDAP (SLDAP)



# Directory Threats

---

- Network Routing Information
- Strong Authentication for update
- May need strong auth for read and results  
(ex: e-mail addr, mobilization information)
- Denial of service - substituting Certs and CRLs

# LESSONS LEARNED

# LESSONS LEARNED

---

- X.500 and LDAP Error Messages
- Too many DNs !
- Integrity of Data and Signed Operations
- Clock Synchronization
- DER vs BER on the wire
- X.500 1988/1993 Incompatibility
- Other Issues

# X.500 Error Messages

---

- Difficult to isolate precise error
- 1993 X.511 defines 40 errors:
  - 3 abandon errors, 6 attribute errors
  - 4 name errors, 1 referral error
  - 13 service errors, 7 update errors
  - 6 security errors

# LDAP V2 Error Messages

---

- Difficult to isolate precise error
- LDAP V2 defines 34 errors and optional string
  - 5 security errors
  - optional string can help, but
  - optional string is not standardized

# Too many DNs !

---

- DirectoryBindArgument.credentials.strong.certification-path.userCertificate.subject
- DirectoryBindArgument.credentials.strong.name
- DirectoryBindArgument.credentials.strong.bind-token.name
- DirectoryBindResult.credentials.strong.certification-path.userCertificate.subject
- DirectoryBindResult.credentials.strong.name
- DirectoryBindResult.credentials.strong.bind-token.name

# Integrity of Data and Signed Operations

---

- How is the data stored? (certs decoded, re-encoded)
- How is the data provided to the client? (string, ASN.1, binary, DER, BER)
- How is a signed operation or result preserved as it flows through the system?

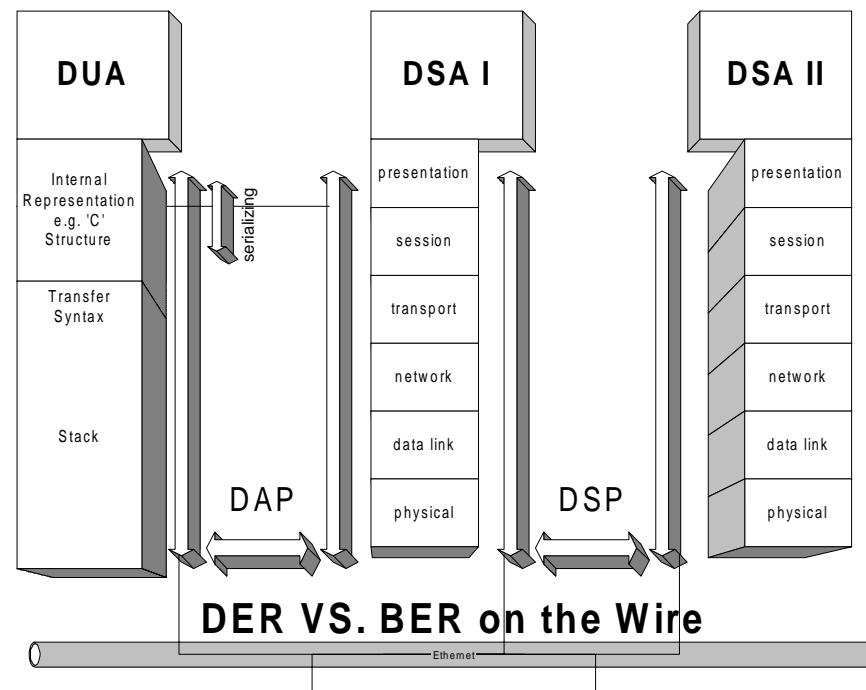
# Clock Synchronization

---

- Clocks must be synchronized for both
  - X.511 Signed DAP Operations and Results
  - X.518 Distributed Operations (DSP)

# DER vs. BER on the wire

OSI 7 Layer Model



# X.500 1988/1993 Incompatibility

---

- Service Control options are encoded as a Bitstring. The encoding of a bitstring includes the number of unused bits in the last octet of the Bitstring.
- In 1988, there are 5 Service Control options (three unused bits).
- In 1993, there are 7 Service Control options (one unused bit).
- Therefore, signature verification fails.

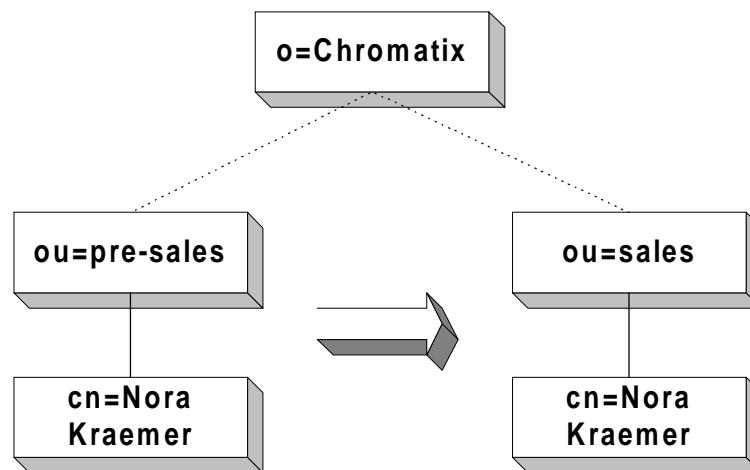
# X.500 1988/1993 Incompatibility (2)

---

- The 1993 X.500 standards writers should have allowed for backward compatibility. Decoding and re-encoding is assumed. That is why DER is used.
- OR-- The PDU should be kept in tact off the wire, and shouldn't be decoded then re-encoded to validate the signature (1997 X.500)
- OR-- Version numbers should be used when changing syntaxes. But, this may force having multiple versions of encoders and decoders.

# Other Issues

- Multi-Component RDNs, ordering of
  - c=us@o=Chromatix@cn=Dave Bernstein +l=Columbia, Md
- Dynamic Schema Discovery
- Multivalued Attributes - client may assume single value, no ordering, admin prob
- LDAP V3 needs more work in the area of strong authentication
- LDAP Schema Issues - defining own attributes; v2 certs passed as string, binary
- Dynamic Nature of Organizations



# SAFEPAGES DIRECTORY SUITE



# SafePages Directory Suite

---

- SafePages Security Features
- SafePages Components
  - SafePages Architecture
  - SafePages Directory Access API
  - SafePages Directory Web Access Gateway
- SafePages Interoperability

# SafePages Security Features

---

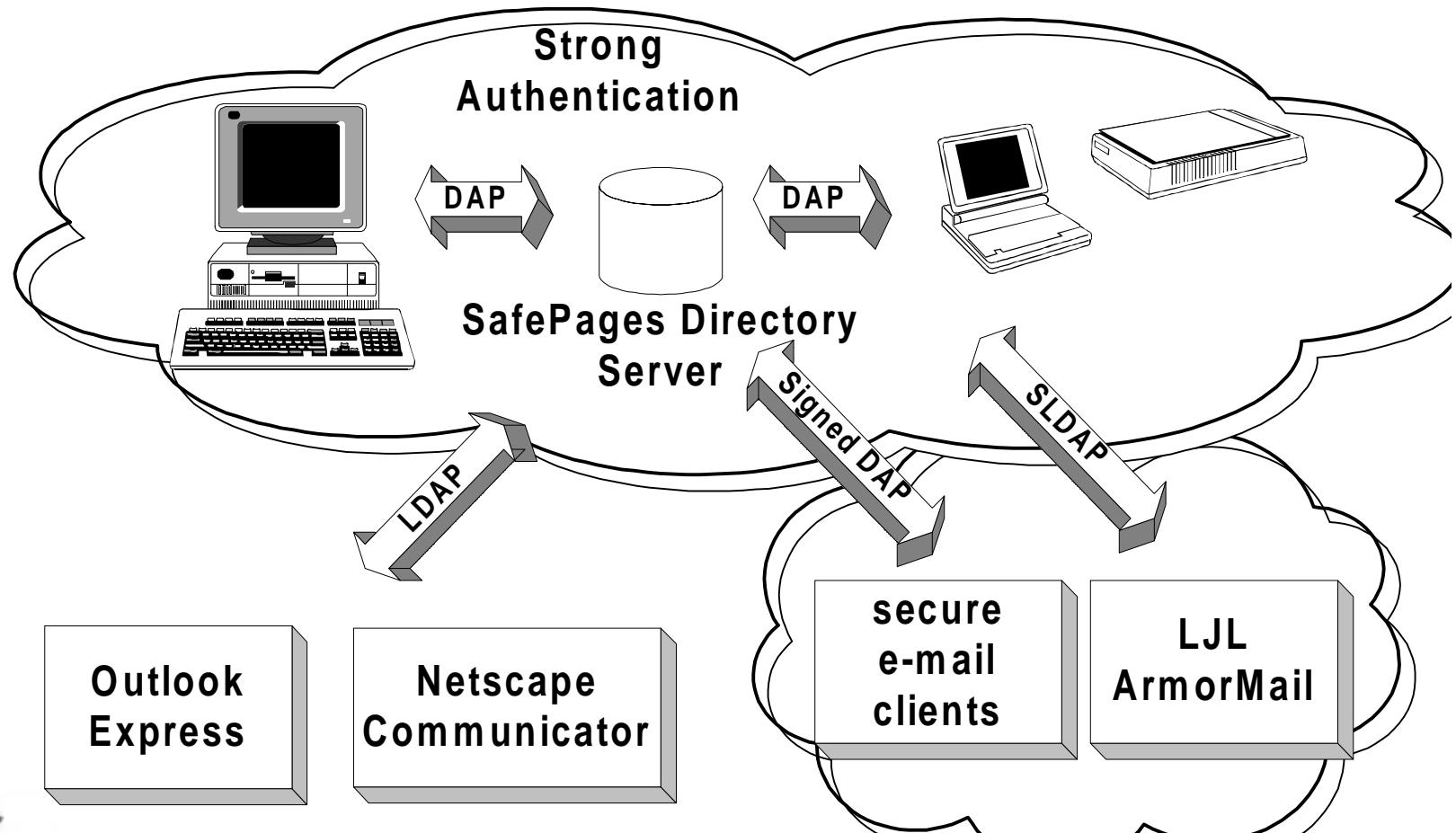
- Signature Algorithms: RSA, DSA
- FIPS 140-1 Level 2 devices
- Hashing Algorithms: SHA-1, MD5
- V1/V3 Certificate Support
- V1/V2 CRL Support
- X.511 Signed DAP Operations, Results / X.501 ACIs
- X.518 Signed DSP, X.525 Signed DISP
- Bulk loading tools
- Platforms - Solaris, HPUX, NT, Windows 95/98 and SCO for Administrator and API

# SafePages Components

---

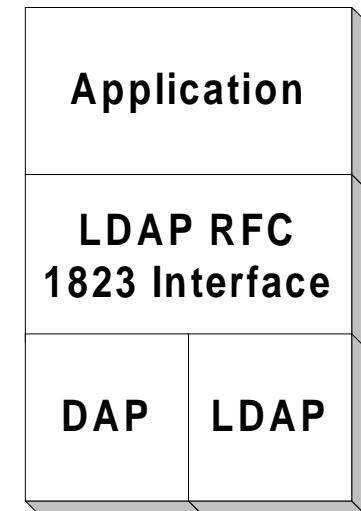
- **SafePages Directory Administrator**
  - Robust management front-end to any LDAP or X.500 Directory
- **SafePages Directory Server**
  - Flexible, high performance, secure LDAP and X.500 server
- **SafePages Directory Access API**
  - ‘C’ development library that allows directory-enabled applications to use both LDAP and DAP
- **SafePages Web Access Gateway**
  - Allows directory access via web browsers

# SafePages Architecture

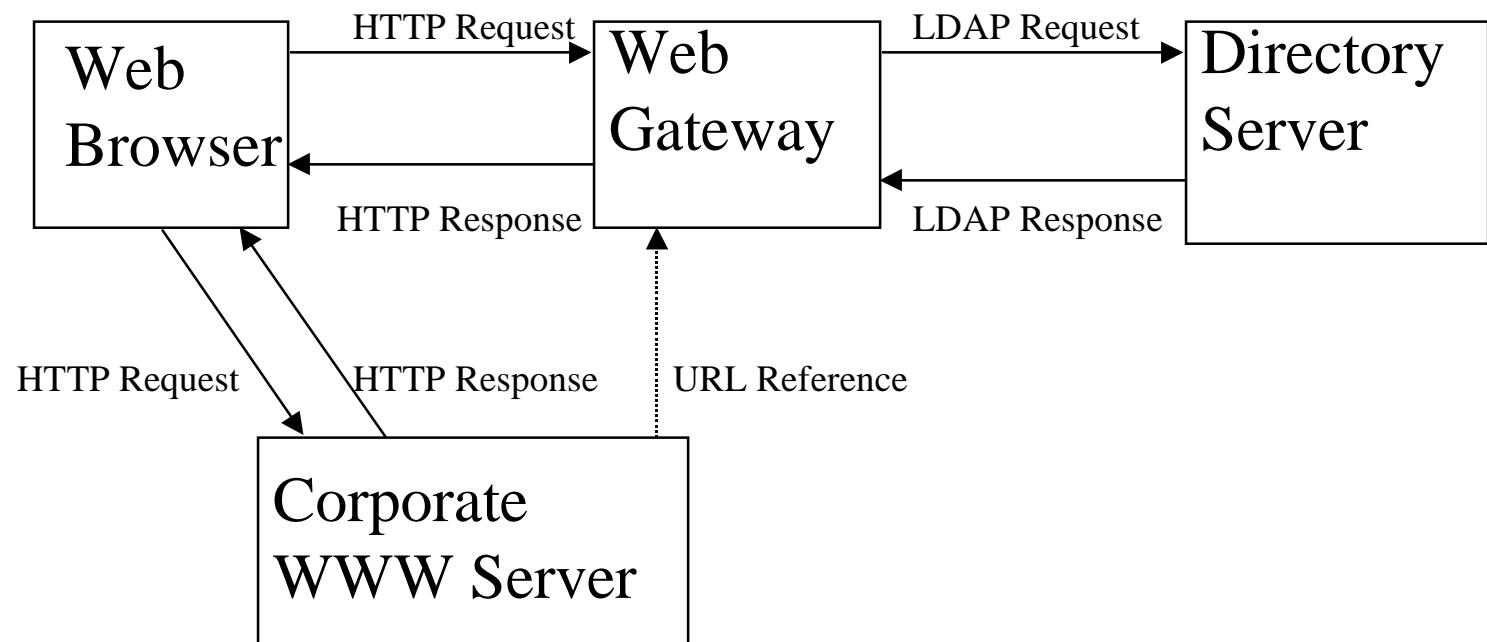


# SafePages Directory Access API (XdAPI)

- Well known LDAP C interface over DAP or LDAP
- Strong Authentication Support on directory operations and results
- Any application written for LDAP can easily support strong authentication using DAP
- Interoperability testing with SafePages, Nexor, Netscape, DCL, and others



# SafePages Directory Web Access Gateway



# SafePages Interoperability

---

- X.500/DAP
  - DMS Clients - Lotus, Microsoft, ESL, Raytheon
  - DCL, Nexor, OpenDirectory
  - CDC, Isocor, ICL, ESL
- Internet/LDAP
  - Netscape
  - SPYRUS S<sup>2</sup>CA (Certification Authority)
- Supported Schema
  - DMS Baseline, NSA SDN.701/702, ACP 120/133, LDAP (incl. inetOrgPerson), Entrust Schema